# Coalition Network Defence Common Operational Picture

**Luc Beaudoin, Marc Grégoire, Philippe Lagadec,**
**Julie Lefebvre, Eric Luiijf, Jens Tölle**
Contact Author: Jens Tölle
Fraunhofer FKIE, Neuenahrer Str. 20,
53343 Wachtberg, Germany

luc.beaudoin@ps-sp.gc.ca, marc.gregoire@drdc-rddc.gc.ca, philippe.lagadec@nc3a.nato.int,
julie.lefebvre@drdc-rddc.gc.ca, eric.luiijf@tno.nl, jens.toelle@fkie.fraunhofer.de

## *ABSTRACT*

*A Coalition Network Defence Common Operational Picture (CNet-D COP) has been identified as a future capability to support cyber defence in coalitions. A CNet-D COP is composed of two aspects of information assurance: secure communications for the sharing of information in a coalition environment and federated cyber situational awareness (SA). The NATO IST-081/RTG-039 task group is focusing on the cyber situational awareness that pertains to a coalition network environment. This paper presents the CNet-D COP concept along with the current results of the NATO IST-081/RTG-039 task group. This paper includes the current situation, followed by a proposed solution for a coalition-wide approach to a network defence COP. In addition, use cases and a scenario are described to illustrate the wider CNet-D COP concept.*

## 1.0 OVERVIEW

Coalition interoperability is of key importance to NATO. There is momentum in NATO for increased coalition information sharing, such as the use of Multilateral Interoperability Program (MIP) and its information exchange data model, to facilitate the establishment of coalition Common Operational Pictures (COPs). Cyber Defence (CD) plays a vital part in military operations, which requires a COP to have situational awareness (SA) and present critical CD information. Cyber warfighters need a coalition-wide COP to facilitate the sharing of Cyber Defence information concerning command, control, communication, computers, combat systems, and intelligence (C5I) from each coalition nation. *A Coalition Network Defence (CNet-D) COP is a means of sharing, assessing, and displaying Cyber Defence information across coalition boundaries so that it may be easily accessed and quickly understood [1].*

The benefits of a CNet-D COP capability could be:

- a clear SA picture made possible by collective, shared CD information;
- resource efficiencies with respect to information assurance, people and processes;
- synchronization of CD activities in real-time.

Several nations have begun developing their own Network Defence COPs. These national Net-D COPs can support the development of a common CNet-D information model, and towards this goal, the NATO RTO activity IST-081/RTG-039 task group is addressing research, technological, and implementation issues related to a CNet-D COP.

The objective of this paper is to present both challenges and the CNet-D COP concept along with the current results of the NATO IST-081/RTG-039 task group. The goal of the task group is to advance research and technology in CD and bring CD SA a step forward. CNet-D COP requires the fusion of data

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

| | | |
|---|---|---|
| 1. REPORT DATE<br>**NOV 2010** | 2. REPORT TYPE<br>**N/A** | 3. DATES COVERED<br>**-** |

4. TITLE AND SUBTITLE
**Coalition Network Defence Common Operational Picture**

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
**Fraunhofer FKIE, Neuenahrer Str. 20, 53343 Wachtberg, Germany**

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADA564697. Information Assurance and Cyber Defence (Assurance de l’information et cyberdefense). RTO-MP-IST-091**

14. ABSTRACT

**A Coalition Network Defence Common Operational Picture (CNet-D COP) has been identified as a future capability to support cyber defence in coalitions. A CNet-D COP is composed of two aspects of information assurance: secure communications for the sharing of information in a coalition environment and federated cyber situational awareness (SA). The NATO IST-081/RTG-039 task group is focusing on the cyber situational awareness that pertains to a coalition network environment. This paper presents the CNet-D COP concept along with the current results of the NATO IST-081/RTG-039 task group. This paper includes the current situation, followed by a proposed solution for a coalition-wide approach to a network defence COP. In addition, use cases and a scenario are described to illustrate the wider CNet-D COP concept.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **SAR** | **18** | |

concerning military operations; information assurance (IA); network management; network security; and command and control. This fusion would enhance the understanding and awareness of network and security management within coalition network operations. A critical step is defining commonalities across national information models for CD SA. Ultimately, the results could influence future international standards or de facto standards in this area. This paper highlights the use cases and challenges in developing and deploying a CNet-D COP system. Based upon these needs, a CD information model and supporting information sharing requirements are derived.

## 2.0 CURRENT SITUATION

Understanding how the military operational community currently shares CD information with coalition partners is a step in capturing requirements. The NATO IST-081/RTG-039 task group is capturing the current operational situation by interviewing the national military operational communities and leading two syndicates at recent NATO Cyber Defence workshops. While the focus is on the types of CD information currently being shared by nations and the sharing agreements, the task group is also looking at gaps, limitations, and constraints resulting from policy, technology, trust, and/or regulations in current practices.

Currently, few military communities share CD information externally. Those who share do so in relatively simple and non-automated forms such as by phone, email, or through web portals. The information more commonly shared is high-level knowledge about incidents, threats, vulnerabilities, and exploits. At the moment, few international agreements exist for sharing CD information. Typically they are bilateral (not multinational) in nature and do not seem to be used to their full extent. CD information sharing is done mostly on requests or during a crisis.

There are examples of communities that share some CD information to build knowledge and for early warning indication. One example is the Internet Storm Center (ISC) run by SANS Institute, which was formed to assist with keeping security professionals aware of the fast paced changes in vulnerabilities, patches, hacks, worms, Trojans and threats in general. The ISC relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public. It succeeds through active participation of people who use firewalls and intrusion detection systems and who understand how sharing the data from those systems is a powerful way to help themselves and the entire Internet community. Internet Protocol (IP) address obfuscation is possible when submitting data. ISC publishes an INFOCON status and reports top scanned ports, top sources of attacks, country reports, trends, etc.

The military operational CD community agrees that there are benefits to CD information sharing, currently there are too many impediments to be practical; these challenges include:

- Legal – ownership of data, civilian privacy concerns
- Technical – automated cross-domain solutions, communication methods, interoperability
- Security – classification/sensitivity of CD information
- Personnel – insufficient training and lack of resources
- Procedural – sharing is not a priority
- Trust – embarrassment, history, privacy

- National – policies, value determination, revealing operational details (vulnerabilities, architecture, internal products)

- Volume and quality of data

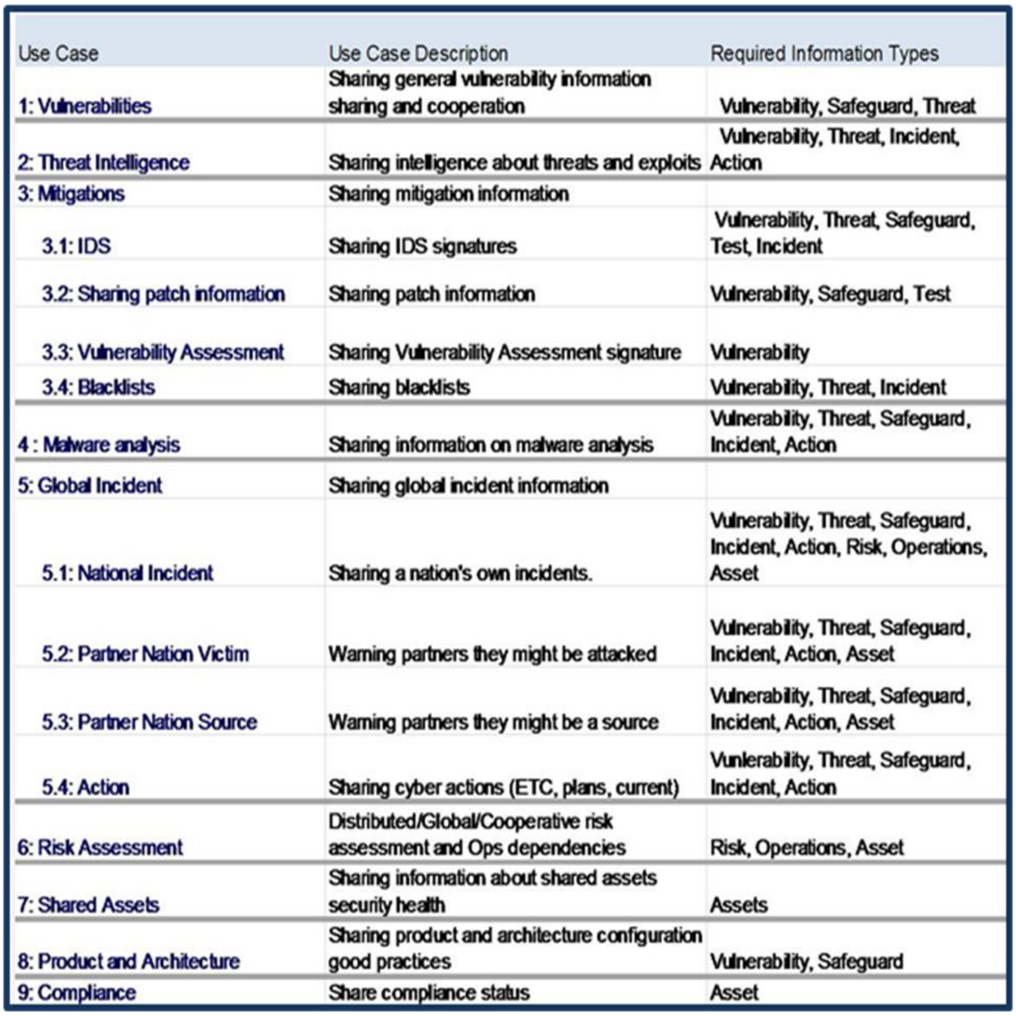
# 3.0 USES CASES, SCENARIOS AND EVENT FLOW

Enhancing coalition cyber defence and cyber intelligence information sharing are key CNet-D COP objectives. Requirements, solutions, and operational deployments depend on the development of realistic uses cases, scenarios, and event flows. In addition, these uses cases and scenarios for CD information sharing require a number of information types and standards.

## 3.1 Use Cases

CNet-D COP use cases must encompass sharing common cyber threat information, identifying coalition cyber assets, and identifying cyber events that increase risk to a coalition or nation.

Table 1. Use Cases and Information Types



| Use Case | Use Case Description | Required Information Types |
|---|---|---|
| 1: Vulnerabilities | Sharing general vulnerability information sharing and cooperation | Vulnerability, Safeguard, Threat |
| 2: Threat Intelligence | Sharing intelligence about threats and exploits | Vulnerability, Threat, Incident, Action |
| 3: Mitigations | Sharing mitigation information | |
| 3.1: IDS | Sharing IDS signatures | Vulnerability, Threat, Safeguard, Test, Incident |
| 3.2: Sharing patch information | Sharing patch information | Vulnerability, Safeguard, Test |
| 3.3: Vulnerability Assessment | Sharing Vulnerability Assessment signature | Vulnerability |
| 3.4: Blacklists | Sharing blacklists | Vulnerability, Threat, Incident |
| 4 : Malware analysis | Sharing information on malware analysis | Vulnerability, Threat, Safeguard, Incident, Action |
| 5: Global Incident | Sharing global incident information | |
| 5.1: National Incident | Sharing a nation's own incidents. | Vulnerability, Threat, Safeguard, Incident, Action, Risk, Operations, Asset |
| 5.2: Partner Nation Victim | Warning partners they might be attacked | Vulnerability, Threat, Safeguard, Incident, Action, Asset |
| 5.3: Partner Nation Source | Warning partners they might be a source | Vulnerability, Threat, Safeguard, Incident, Action, Asset |
| 5.4: Action | Sharing cyber actions (ETC, plans, current) | Vunlerability, Threat, Safeguard, Incident, Action |
| 6: Risk Assessment | Distributed/Global/Cooperative risk assessment and Ops dependencies | Risk, Operations, Asset |
| 7: Shared Assets | Sharing information about shared assets security health | Assets |
| 8: Product and Architecture | Sharing product and architecture configuration good practices | Vulnerability, Safeguard |
| 9: Compliance | Share compliance status | Asset |

A set of identified operational use cases, shown in Table 1, require specific information types including vulnerability, safeguard, threat, incident, test, action, asset, risk and operations. As an example of the operational benefits of the CNet-D COP approach, the next subsections highlight use cases 2, 3, 6, and 7. The CNet-D COP capability is not only a solution and way ahead for international coalitions, but also for national situational awareness.

### 3.1.1 Use Case: Share Cyber Threat and Mitigation Information

Sharing cyber threat and mitigation information, a combination of Use Case 2 and 3, requires coalition partners share information regarding adversarial cyber tactics, techniques, and procedures (TTP). Coalition partners could mitigate adversary TTPs such as exploiting software or infrastructure vulnerabilities through network, local, or social (e.g., phishing) vectors, by sharing cyber defence information in the form of software patch information, defence strategies, malware or intrusion detection system (IDS) signatures, attack correlation patterns, or domain blacklists. When a nation identifies cyber defence information useful to coalition partners, the nation can issue a report to the CNet-D COP. As a result, each nation registered with the CNet-D COP receives a notification on this new defence information and can choose to utilize this intelligence.

In addition to sharing threat intelligence information, the coalition must standardize on the information types and contents of cyber defence data. For example, one type of defence information, a safeguard alert, could warn partners to be on the lookout for a certain pattern in network traffic. This alert must contain information regarding the network data pattern (e.g., source, destination, port, protocols). In addition, the inclusion of a formatted IDS rule (preferably using a recognized standard, such as using the Sourcefire Snort IDS rule format) would allow for a faster coalition-wide response time.

### 3.1.2 Use Case: Identify Shared Cyber Assets

Use case 7 represents the identification of shared cyber assets, where coalition members rely upon joint assets such as communication links, systems, and services that are crucial for mission success. For example, communication links (e.g. wired networks, relays, mobile networks, satellite links) are the channels for the exchange of critical mission orders, imagery, and other information. When link disruption or degradation occurs, affected armed forces must be able to quickly locate nearby, active links to continue the current mission. Similar requirements apply to systems and services—coalition forces must know which cyber assets are available and trusted.

### 3.1.3 Use Case: Identify Cyber Events Increasing Coalition Risk

Identifying cyber events that increase coalition risk, where the loss or compromise of a cyber asset by one nation poses a risk to the entire coalition, represents Use Case 6. Certain events, such as attacks, loss of power or technical failure (even when a redundant system takes over), may either have a critical impact on or be a critical risk factor to coalition cyber operations; nations must be informed of these risk factors.

The CNet-D COP helps to evaluate the impacts of such events by alerting nations to a loss of cyber asset availability, limited risky operating capability, or integrity. To mitigate this risk, nations must be aware of assets that have operational dependencies and the events that affect these assets. Once a coalition member is notified of a risk event, it is each nation's obligation to evaluate the impact of the event on that nation, their assets, and their coalition responsibilities.

## 3.2 Information Types and Standards

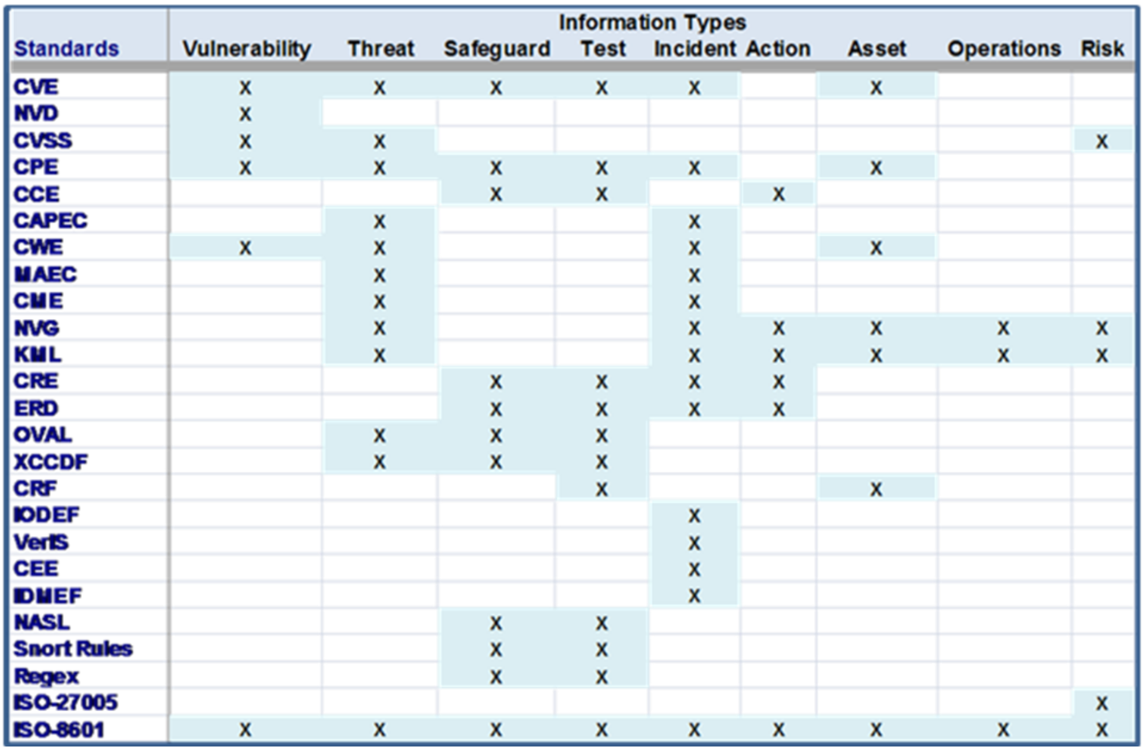
Each use case depends on various categories of shared information; these critical information types are described and tabulated in Table 2.

Table 2 - Main information types

| Type | Description |
|---|---|
| Vulnerability | The category “Vulnerability” includes all reference information related to vulnerabilities and weaknesses which can be shared between coalition partners, such as general vulnerability characteristics provided by the National Vulnerability Database (NVD) [3].<br>It also includes information about actual vulnerability instances detected on assets when this information can be shared between coalition partners.<br>Global metrics, statistics and trends about detected vulnerabilities are also covered by this category. |
| Threat | The category “Threat” includes all information related to various threat actors such as malware, worms, viruses, exploits and attack patterns. It also covers information about known attack sources. |
| Safeguard | The category “Safeguard” includes all information related to safeguards, counter-measures, mitigations and possible responses to a cyber incident. This covers patches, security updates, workarounds, IDS signatures and vulnerability assessment signatures. |
| Test | The category “Test” includes all information related to test results that can be shared between partners in order to improve global knowledge. For example, a Nation may have tested a specific patch or IDS signature against an exploit and may share this result to inform their coalition partners. |
| Incident | The category “Incident” includes information about cyber incidents that have happened in coalition partner networks or on shared coalition assets. These incident reports may be anonymized to enable sharing of information valuable to the coalition while not revealing private information.<br>This category also covers global metrics, statistics and trends about incidents. |
| Action | The category “Action” includes all information about actions taken or planned by one or more coalition partners that may have an impact on the coalition network operations, and its services such as disconnecting a network or stopping a service temporarily to respond to an incident. Sharing this type of information is relevant when other partners depend on such assets. |
| Asset | The category “Asset” includes all information related to the global ICT infrastructure of each coalition partner, such as network topology, computers and network devices. Sharing this type of information is relevant when other partners depend on these assets. |
| Operations | The category “Operations” includes all information related to missions, operations and business services. This also includes the description of dependencies between these objects and the ICT infrastructure. |
| Risk | The category “Risk” includes all metrics related to risk assessment, usually based on the dependencies between operations and the IT infrastructure. |

Leveraging existing standards will help ensure interoperability for information sharing between coalition partners. Table 3 lists relevant standards for each type of information considered in CNet-D COP (see references [2-26]). Due to the number and progress of applicable standards activities, this list must be updated before any specification and implementation of CNet-D COP interfaces.

Table 3 - Standards for CD information sharing



| Standards | Information Types | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Vulnerability | Threat | Safeguard | Test | Incident | Action | Asset | Operations | Risk |
| CVE | x | x | x | x | x | | x | | |
| NVD | x | | | | | | | | |
| CVSS | x | x | | | | | | | x |
| CPE | x | x | x | x | x | | x | | |
| CCE | | | x | x | | x | | | |
| CAPEC | | x | | | x | | | | |
| CWE | x | x | | | x | | x | | |
| MAEC | | x | | | x | | | | |
| CME | | x | | | x | | | | |
| NVG | | x | | | x | x | x | x | x |
| KML | | x | | | x | x | x | x | x |
| CRE | | | x | x | x | x | | | |
| ERD | | | x | x | x | x | | | |
| OVAL | | x | x | x | | | | | |
| XCCDF | | x | x | x | | | | | |
| CRF | | | | x | | | x | | |
| IODEF | | | | | x | | | | |
| VerIS | | | | | x | | | | |
| CEE | | | | | x | | | | |
| IDMEF | | | | | x | | | | |
| NASL | | | x | x | | | | | |
| Snort Rules | | | x | x | | | | | |
| Regex | | | x | x | | | | | |
| ISO-27005 | | | | | | | | | x |
| ISO-8601 | x | x | x | x | x | x | x | x | x |

## 3.3 Example Scenario and Event Flow

An example scenario and event flow comparison for current and CNet-D COP-enabled operations highlight its benefits and disadvantages. The scenario, *iWar/Cyber War*, depicts an incident-detection situation requiring sharing attack patterns where each affected coalition nation is operating independently with no shared assets. In this scenario, a coalition nation is attacked by a large botnet creating a distributed denial of service (DDoS) across multiple sectors (i.e., critical infrastructure components, government, banks, media). Hostile nation groups motivated by political tensions undertake this nation-wide attack. The attack quickly extends to other coalition nations. These nations are able to leverage multiple critical information-based infrastructures to help identify and detect the various attacks indicating a widespread DDoS.

**Current Event Flow**: Currently, each nation under attack must individually initiate the event flow below. The lack of international coordination results in the replication of complex, time-consuming tasks.

1. The botnet starts attacking a single Country A. Primarily through manual processes.
2. Country A organizations detect a DoS attack on their critical information-based infrastructures.
3. Major ISPs in Country A take independent measures to respond to attacks.
4. ISPs report to Country A’s national computer security incident response team (CSIRT).
5. Country A CSIRT report a large-scale attack. Potential sources, targeting trends identified.
6. CSIRTs notify partners, issue mitigation strategies (firewall rules, signatures, IP blacklists)
7. Mitigation implementations begin. (critical infrastructure components, government, banks, media)
8. Country A National CSIRT informs other countries National CSIRTs.
   a. Human reports- no specific template;
   b. E-mail and Internet may not be available, only telephone, fax, and out of band communications International contacts may be called one at a time.

9. Media report the news and end-users get informed.

**CNet-D COP Enabled Event Flow**: When the CNet-D COP is enabled, situation awareness and coordination across boundaries is automated and shared; resulting in early warning and faster response. The coalition event flow is detailed below:

1. The botnet starts attacking a single Country A.
2. National CND COP sensors detect a DDoS attack and generate alerts.
3. Activity rise automatically shared as a trend indicator with the coalition through CNet-D COP.
4. Alerts and trends correlated by Country A CND capabilities- escalates DDoS attack as incidents.
5. Potential sources, targeting trends identified by CSIRT.
6. CNet-D COP shares information with countries and major national players.
7. CSIRTs notify partners to identify the attack status and characteristics. National CSIRTs in coalition use the CNet-D COP to share their situation assessment and coordinate actions.
8. Country A major players (ISPs, critical infrastructure components, government, banks, media) implement mitigations. CNET-D COP reports status to national CSIRTs.
9. CSIRTs in all involved nations coordinate mitigation strategies through CNet-D COP.
10. The botnet targets other coalition countries. Attacks are quickly detected and mitigated.
11. Media report the news and end users are informed.
12.

Clearly the CNET-D COP enabled approach significantly enhances international situational awareness; facilitating the timely assessment of a large-scale DDoS-attack. In addition, the event correlation and information sharing automation provides early warning and faster reactions for other nations. Finally, the CNET-D COP, designed with standard formats, will automatically consolidate information in an overview; enabling faster and more effective situation assessment and response.

Although the CNet-D COP is a valuable coalition asset, several negative factors must be taken into account when considering COP adoption. These factors include the cost of development, political pushback, potential legal issues related to sharing sensitive information (e.g., IP addresses), potential over reactions, and the CNet-D COP vulnerability to DDoS.

## 4.0 PROPOSED SOLUTION

The proposed CNet-D COP solution consists of several key components: coalition-wide situational awareness, coalition-wide standards, a common information model, and an appropriate architecture for the exchange of information. Mutual policies must be initiated to agree on a shared set of data. International policies must be set up to permit data exchange.

The following is a suggested list of CD information that can be shared without too many constraints:

- Points of contacts: Who is on duty and can be reached in case of problems
- Reference information about vulnerabilities, patches, malware, and exploits. This information should be focused on the specific coalition needs regarding to its cyber assets. There is no need to duplicate publicly available sources.
- National security policy information
- Black lists of known hostile IPs, domains, URLs, e-mails, or nicknames.
- File hashes (e.g. MD5 hashes) that can be used to identify both malware as well as trusted software

- IDS signatures
- National metrics and trends
- Useful tools and publications
- National R&D initiatives
- CD-related questions and requests between coalition partners

Additional information can be exchanged based on jointly-defined information policies.

## 4.1 Appropriate Architecture

Military, government, and civil networks are typically equipped with different kinds of security tools. Depending on the different nation and organization-specific procedures and policies, the structure of the network domain and its security architecture may vary significantly.

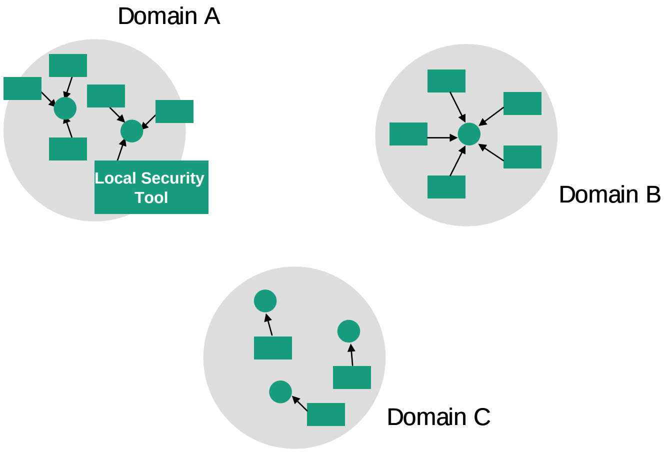


**Figure 1: Different approaches for network domains and their security architectures**

Figure 1 illustrates different architecture approaches. Domain A embeds a set of local security tools (e.g., IDS/Intrusion Prevention System (IPS) with distributed sensors), represented by rectangles. Several central nodes (e.g., consoles, national Net-D COPs) represented by dots gather data (e.g., event messages, statistics, warning messages). The central nodes may or may not have connections to exchange data. In domain B, a single central instance is used to achieve domain-wide situational awareness. Here, redundancy is needed to avoid single points of failures. In domain C, a fully distributed approach is used.

A typical network topology for coalition operations is a set of independent domains connected to a coalition backbone using gateways or so-called Interoperability Points. Figure 2 shows two different approaches to exchange CD-related information between coalition partners.

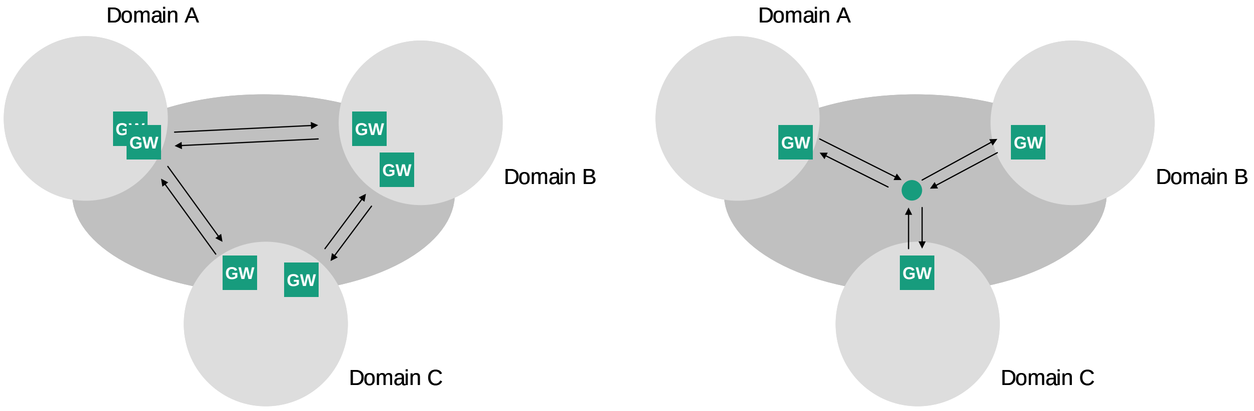


**Figure 2: Different approaches to exchange data in coalitions**

On the left-hand side of Figure 2, we see dedicated communication channels for the exchange of information between specific coalition partners. An advantage of this approach is the ability to nationally decide which kind of information can be exchanged with a specific coalition partner. In contrast, the management of this structure is complex and error-prone. In case of a change in coalition membership, all domains have to update their communication relations. Thus, there is a huge management overhead for a large amount of 1-to-1 communication links.

On the right-hand side of Figure 2, a centralized node is shown, which is responsible for communicating with each of the national domains. Only one interface standard has to be implemented by the nations. The amount of communication links is small (only one per nation), and adding a new coalition partner or removing a coalition partners is easy to handle without bothering each coalition partners. Again, in this concept additional redundancy is needed to avoid a single point of failure. A major challenge in this second approach might be to find a coalition-wide information exchange policy that is acceptable to all coalition members.

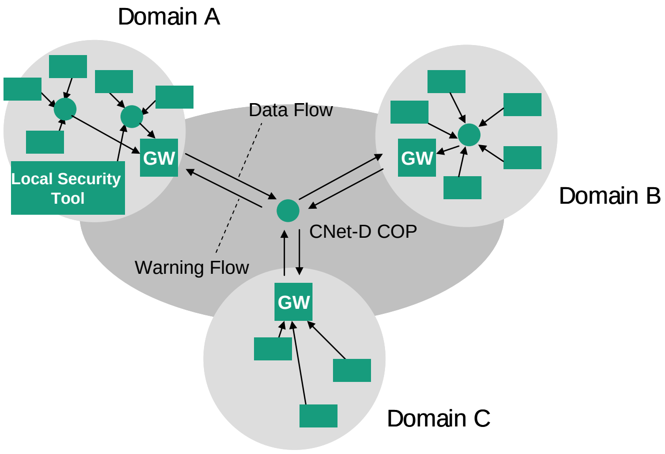


**Figure 3: A Potential CNet-D COP Architecture**

Given the two concepts in Figure 2, the centralized approach offers a good and efficient basis for a coalition-wide CNet-D COP. It is a feasible concept with which to offer information sharing capabilities. Only one interface standard has to be defined; only a single standardized information sharing protocol is needed, and there is no need for all coalition partners to agree on interface standards and information sharing policies with every other coalition member. Figure 3 shows the flexibility of the approach. Each national infrastructure is under control of the individual nation and follows national security policies and procedures. The internal structures of the national domains may vary significantly. Each nation may use different tools to supervise its network traffic and the security health status of its networks in order to gain situational awareness about its own domain. The challenge is that national systems may not be interoperable with other nation's systems. In domain A, we see multiple national Net-D COPs, gathering information from their own domain, and offering information to the coalition partners. In domain B, we see a centralized Net-D COP connected to coalition partners. In domain C, we do not have a Net-D COP, but nevertheless we see a set of security tools contributing directly to the coalition-wide CNet-D COP.

Every nation maintains a gateway (GW) which converts messages into a coalition standard format. These gateways are fully under national control. Another task of the gateways (message sanitization) is explained later in this section.

The CNet-D Cop is operated by a trusted organization. This may be a trusted coalition member or a supra-national organization (e.g., a NATO operational agency). Figure 3 shows directional communication links from the national gateways to the CNet-D COP as well as in the opposite direction. The concept is to gather statistics, warning messages, and event messages from the national domains, and to offer warning messages (alert feedback) to the nations. The distribution of the warning messages inside nations is not shown in this figure.

## 4.2 The CNet-D COP Information Model

The gateways and the central CNet-D COP instance have to agree on information exchange formats and a common information model in order to ensure interoperability. As an example, the Internet Engineering Task Force (IETF) standardized the Intrusion Detection Message Exchange Format (IDMEF) [21] to define a standard for product vendors to exchange intrusion detection related event messages.

This section contains an overview of an initial CNet-D COP information model. This first version of the model is partial and should be considered as work in progress. It will be refined and extended in the future by the task group in order to guide future work on the specification and implementation of the COP.

The COP requires a CD information model that meets the needs of the coalition and supports the use cases as described in section 3. Wherever possible, the COP will leverage existing standards. In section 3.2, a list of relevant standards has been suggested, in relation with all information types derived from CNet-D COP use cases.

The task group has identified at least three existing data models which have been designed to build the CD COP of a nation for situational awareness:

- the Network Defence data model in the US,
- the Joint Network Defence Management System (JNDMS) data model in Canada,
- and the Consolidated Information Assurance Picture data model in NATO.

Because all these models can be quite complex and cover a broader scope than CNet-D COP, it has been decided to derive the information model requirements from the use cases identified in section 3, rather than to use one of these data models directly and to remove unnecessary parts. However, all these data models provide very relevant inputs and can be leveraged to guide future work on the specification and implementation of the CNet-D COP.

Since the CNet-D COP is designed to operate in a centralized, coalition environment, it will have to be updated regarding each nation's information sharing policies and restrictions. This requires that all information sent to and from the COP must contain certain metadata to describe how it must be handled. Minimally, each piece of CD information must indicate the contributing nation, how and with whom that data can be shared, along with some general prioritization indicating how urgently other nations should react.

Therefore, CNet-D COP data can be grouped into two top-level categories: information sharing requirements metadata and CD information (Figure 4).

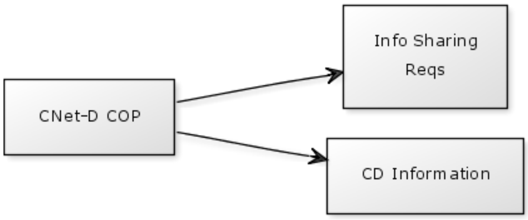


**Figure 4: CNet-D COP High-level Information categories**

### 4.2.1 Information Sharing Requirements Metadata

Regardless of which type of CD information is shared, some metadata must be associated with each piece of CD information to describe how it must be handled. Each CD record must contain an indication of the data's priority, which nation is providing the data, to which nations the data is releasable, and the dates when the data is applicable (Figure 5, right-hand side). For example, this allows the United States to inform Canada, Germany, and The Netherlands to be on the lookout for a high priority cyber threat from 1-5 January 2011.

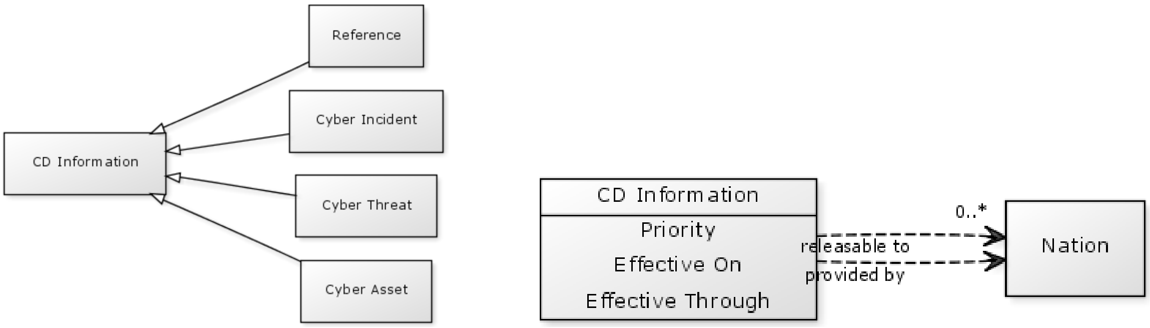


**Figure 5: CND Data Types (on the left) and CND Data Decomposition (on the right)**

### 4.2.2 CD Information

CD information is any data that may be of use to coalition nations in helping them defend against cyber threats. In the context of CNet-D COP, this data corresponds to the main information types identified in section 3.2: vulnerabilities, threats, safeguards, tests, incidents, actions, assets, operations, and risks.

Currently, the initial version of the CNet-D COP information model described in this paper focuses on four classes of CD information: cyber asset, cyber threat, cyber incident, and reference data. It will be extended in the future to cover all required information types.

- Cyber asset data provides information regarding the shared cyber assets (e.g., systems, services, communication links) provided by coalition nations (Figure 5, left-hand side).

- Cyber threat data consists of any intelligence concerning the detection or mitigation of any cyber threat or adversary.
- Cyber incident data detail events that affect cyber assets and increase national or coalition risk.
- Reference information provides associations with known vulnerabilities, intrusion detection, and malware detection signatures.

### 4.2.3 Cyber Assets

Nations providing shared cyber assets must register these cyber assets with the COP for other nations to view and utilize, if permitted.

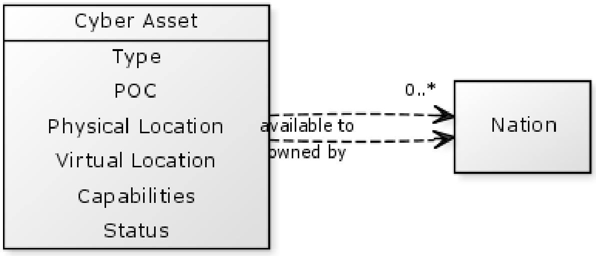


**Figure 6: Cyber Asset Model**

Each cyber asset entry contains data reflecting the asset's type, status, location, and offered services (Figure 6). In addition, the CNet-D COP needs to know the nation responsible for the asset, a point-of-contact, and any usage restrictions (e.g., operational area, operational hours, nation-based usage).

A cyber asset can be one of a number of types. The more common assets include communication links for data or voice, geo-services, Internet access or e-mail. Warfighters may additionally require specific, C5I capabilities such as Friendly Force Tracking (FFT), command and control (C2), intelligence, or coalition COP services.

### 4.2.4 Cyber Threats

Nations and systems are always threatened. Threats may come from the environment, friendly, or enemy forces. Regardless of the actual form of the threat information, it is important that the CNet-D COP disburses the cyber status reports to all coalition nations. If one coalition partner is threatened, the coalition is threatened.

Currently there exists no standard for expressing the full range of cyber threat or adversarial tactics, techniques, and procedures (TTP), apart from the few ones identified in section 3.2. To share such threat information, the CNet-D COP may support unstructured reports. Human analysts are required to read and process these freeform reports. If a nation has additional data to add to a report, they are able to do so by submitting a new piece of intelligence data that references the previous submission. As the data is mostly heterogeneous, there is no way for it to be entirely standardized. However, nations should be encouraged to utilize existing information standards, such as CVE to identify exploited vulnerabilities or NVG (NATO Vector Graphics) to identify geo-locations.

### 4.2.5 CD Reference Information

CD reference information comes in many different forms—detection signatures, mitigations, vulnerability data, etc. The CNet-D COP should support at least the following five types of reference information:

vulnerability information, blacklists, attack patterns, intrusion detection signatures, and malware information. (Figure 7).

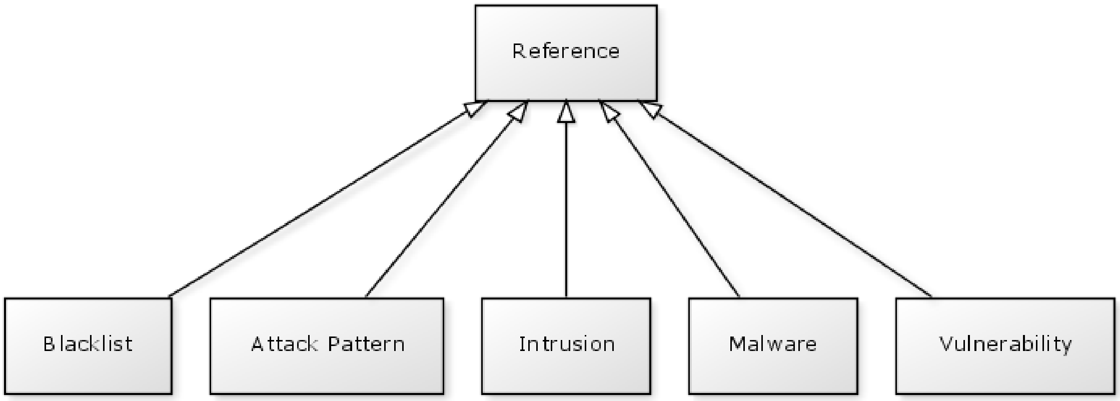


**Figure 7: Cyber Defence Reference Information**

Blacklist data helps nations to identify and block known malicious IP addresses and domains. This data can be used to configure firewalls, DNS, and other servers to block network traffic originating from or going to certain domains. Blacklists also provide analysts with external prioritization information on the network traffic or security reports, as another nation has already associated certain addresses with malicious activity.

Attack patterns are series of events that are indicative of a known attack. At their core, attack patterns are just a sequence of correlated events that represent a more generalized behaviour with a malicious intent. A security information or event manager (SIM or SIEM) typically does this correlation. One example of an attack pattern would be (1) seeing an e-mail with an attachment containing the signature for a known virus, followed by (2) an execution of a file and (3) a subsequent privilege escalation request on a system belonging to the e-mail's recipient. Further attack indicators may include (4) outgoing beaconing requests to a specific domain, or (5) an increase in local traffic data across specific ports as the virus tries to spread. There is currently no known format for expressing attack patterns. The MITRE Corporation is doing work in developing the Common Attack Pattern Enumeration and Classification (CAPEC) standard, which the COP may leverage for the identification and representation of such attack pattern data.

Intrusion indicators are a class of information that includes intrusion detection system (IDS) signatures and behaviours for both network (NIDS) and host-based (HIDS) intrusion detection system sensors. The intrusion indicators and relevant descriptions may be shared with other nations through the COP. As with malware indicators, nations should share intrusion indicators in a format that allows for rapid deployment of the signatures throughout their networks. The current de facto IDS signature format standard is the rule format used by the Sourcefire Snort IDS.

Malware indicators are signatures that are used to identify viruses, Trojans, backdoors, and rootkits. A nation can load these signatures into their anti-virus (AV) infrastructure to help identify and prevent assets from becoming infected. In addition to the actual detection signatures, nations may include mitigation or removal instructions. To allow for rapid dissemination, the COP should disseminate malware signatures in a format that can be easily loaded into most anti-virus/anti-malware tools. At this time, no signature standard or format has been identified.

Vulnerability information can be submitted to the COP to make nations aware of new vulnerabilities and mitigation (e.g., patch) information. Every year thousands of new vulnerabilities in software products are reported[1]. Some of these products are used to support coalition operations. Each vulnerability record contains a description of the vulnerability, a list of possible mitigation techniques such as patching or configuration changes, *Common Vulnerabilities and Exposures* (CVE) identifiers, *Common Vulnerability Scoring System* (CVSS) threat scores, or listings of affected products named using *Common Platform Enumeration* (CPE) identifiers (Figure 8).

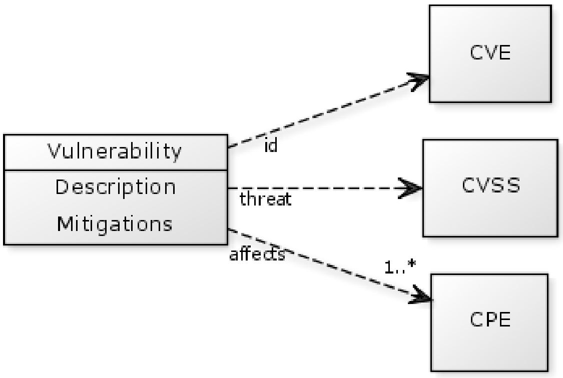


**Figure 8: Vulnerability Reference Information Model**

### 4.2.6 Cyber Incidents

Cyber incidents require the capture of event logs, audit trails, or alerts that affect cyber assets, as well as all information related to the handling of the incident. As some systems and sensors are capable of recording hundreds of different event types at rates that can quickly overwhelm most systems, the CNet-D COP is only concerned about collecting events that increase coalition risk.

In order to identify risk, nations are responsible for sharing events that affect a shared cyber asset. A negative impact might be degraded operations or system or service outages due to attacks, technical problems, or environmental conditions (e.g., sandstorm, lack of power). In addition to providing a list of the impacted cyber assets, nations reporting cyber events should also indicate the time of the event, the type and severity of the impact, and any mitigation notes (Figure 9). The mitigation information makes nations aware of similar assets or capabilities that may exist in other locations or are made available by another nation.

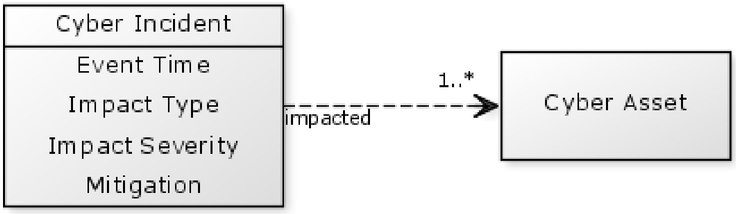


**Figure 9: Cyber Incident Model**

The Common Event Expression (CEE) event standard is aiming to work with vendors to produce events with better data and a more consistent, cross-product format. While CEE is more complex than is required for the CNet-D COP, CEE provides a useful event structure. Coalition adoption of CEE would make it easier for nations to share and correlate events to identify coalition mission risk.

[1] According to the NIST National Vulnerability Database (http://nvd.nist.gov), over 5600 new vulnerabilities were discovered in each 2008 and 2009.

## 4.3 Information Sharing

The justification for adopting a CNet-D COP is based on the principles of war (such as security, flexibility, concentration of force, maneuverability, etc.) with the intended outcome that your Observe, Orient, Decide, Act (OODA) loop is quicker than your adversary's. A CNet-D COP should serve to enhance the information available in the CD OODA loop among coalition partners. Nations share CD information when they have shared network resources, shared operations, or as a "for your information" only. In general, the information exchanged can relate to all phases of the OODA loop (for example, sharing sensor information, sharing fused data, sharing courses of action (COA), and acting on the chosen COA).

The CD data contributed by various nations is only valuable if it can be shared with others. Ideally, all CNet-D COP information could be shared with everyone. Unfortunately, this is not and will never be the case; coalition environments cause many problems with sharing information between various countries. The centralised CNet-D COP infrastructure allows all information to be shared with the coalition partners and distributed only to the nations that the originating nation explicitly permits.

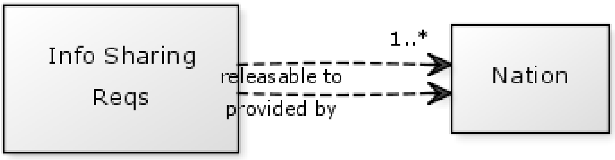


**Figure 10: Information Sharing Model**

To facilitate CD information with as many nations as possible, each nation should register their information sharing requirements with the CNet-D COP. Generally, the sharing requirements are provided by a nation and list the other nations with whom to share the CND data they provide (Figure 10). Each requirement is unidirectional – if `Nation A` shares their data with `Nation B`, `Nation B` is under no obligation to reciprocate by sharing with `Nation A`.

By automating the CD sharing process, the coalition status can be monitored in near-real time with each nation receiving a continual stream of updated asset, threat, incident, and reference data. In addition to the rapid data sharing benefits, other reasons for automating information sharing include addressing the natural human resistance to sharing, handling the large quantities of data, and the potential information complexity.

### 4.3.1 Increase Battle Pace

On the battlefield, there is always incentive to increase the pace of battle. The force that can perform more OODA cycles will have the upper hand and will likely be able to out maneuver and out strategize their opponents. Whether fighting on virtual or actual battlefields, advantages of only milliseconds can be the difference between mission success and mission failure. Automation allows for the removal of humans from the information sharing cycle, thus increasing the rate of CD information sharing amongst coalition forces.

### 4.3.2 Human Resistance to Sharing

In addition to being slower, humans also may have reluctance to share information. Time critical information may not be shared soon enough. Humans could induce delays that lead to mission failure. If CD information sharing requirements can be expressed in rules, computers can quickly evaluate and share information with only certain parties. Letting the system enforce sharing requirements ensure that CD information is quickly shared with only those it is allowed to be shared. Likewise, automation ensures that information is not mistakenly shared with those whom it is not intended.

### 4.3.3 CD Information Overload

Automated CD information sharing shifts the burden of processing and sharing the information to the systems. These systems can efficiently handle multitudes of information more than a human analyst. In addition, unlike their human counterparts, systems are not prone to fatigue, mistakes, or persuasion.

### 4.3.4 CD Information Complexity

Information can become complex quickly. The correlation, aggregation, and identification of threat, incident, and other CD information can introduce nuances and assumptions into the information chain. When interpreting such information, humans are more prone to miss important information or reach improper conclusions based on misunderstood data. Automated systems can overcome such limitations.

## 5.0 FUTURE DIRECTIONS

There are a number of areas which need further research to enable an effective CNet-D COP. Future work of the NATO IST-081 RTG will include:

Refine the information model – The data modelling workshop sponsored in March 2010 brought together a number of key actors for the first time, including data modelling experts from the US, Canada, and NATO. The outcome of this workshop was an increased awareness of various data modelling efforts relevant to a CNet-D COP. The US initiatives in this area will lead to increased adoption of existing data standards and initiation of new ones, and for this reason will have to be tracked closely. Future work will involve identifying the NATO CNet-D COP data model based upon mappings from each countries data models.

Value determination – Research needs to be done about the value determination each country has done in relation to value added by a NATO CNet-D COP to include risk/reward determinations. While many benefits have been identified relating to a NATO level CNet-D COP it would be of value to gather further information about the interest and impediments to establishment as a next step.

Define high-level metrics to be shared – With multiple countries contributing information, further research into options for analysis to include metrics determination and data fusion need to be accomplished. Identification of key metrics, to be shared through a CNet-D COP, which can bring high value to coalition cyber defence, will need to address trust and privacy concerns. Anonymization could address some of these concerns.

Finalize list of suggested standards – Another aspect of rapid development is the formal and de-facto standards emerging in cyber defence. Further inspection, identification and decisions on which standards NATO members might consider need to be made. Recent framework offerings from commercial service providers, to promote increased sharing, will have to be analysed as well. The list of standards for data exchange will be a key aspect of our final recommendations.

Define specifications for a common CNet-D COP interface – Specification details on the interface to the CNet-D COP will have to be developed. These will include such things as XML schemas and web services to enable data exchange through common message formats. Specifications for the interface will enable experimentation with proof-of-concept systems.

Proof-of-concept experimentation – A potential future step could be experimentation using the prototypes currently available within some of the national R&D organizations. Experimentation would support the validation of the specifications being considered for a CNet-D COP system. It would also allow exploration in the area of visualization of cyber defence information, which is still immature.

Identify relevant future stakeholder organizations – Advancement towards the establishment a CNet-D COP will eventually transition away from research and development organizations in favour of implementation bodies. These bodies are also rapidly progressing as warfighter needs are mandating action. Identifying and possibly establishing awareness among these stakeholder organizations will help ensure efforts are coordinated effectively. Progress has already been made in this aspect with the data model workshop held in March 2010.

## ACKNOWLEDGEMENTS

This paper was prepared by members of the NATO-RTO IST-081/RTG-039 task group on Coalition Network Defence Common Operational Picture CNet-D COP. The authors would like to thank all involved persons and organizations for their support and contribution to this paper.

## REFERENCES

[1] L. Genik, J.H. Lefebvre, and M. Froh, *Coalition Computer Network Defence Common Operating Picture Concept*, 13th ICCRTS, Paper 74.

[2] CVE, Common Vulnerabilities and Exposures, http://cve.mitre.org/

[3] NVD, National Vulnerability Database, http://nvd.nist.gov/

[4] CVSS, Common Vulnerability Scoring System, http://www.first.org/cvss/

[5] CPE, Common Platform Enumeration, http://cpe.mitre.org/

[6] CCE, Common Configuration Enumeration, http://cce.mitre.org/

[7] CAPEC, Common Attack Pattern Enumeration and Classification, http://capec.mitre.org/

[8] CWE, Common Weakness Enumeration, http://cwe.mitre.org/

[9] MAEC, Malware Attribute Enumeration and Characterization, http://maec.mitre.org/

[10] CME, Common Malware Enumeration, http://cme.mitre.org/

[11] NVG, NATO Vector Graphics.

[12] KML, Keyhole Markup Language, http://en.wikipedia.org/wiki/Keyhole_Markup_Language.

[13] CRE, Common Remediation Enumeration, http://scap.nist.gov/events/2009/itsac/presentations/day4/Day4_SCAP_Wojcik.pdf

[14] ERD, Extended Remediation Data, http://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_DoD_Wojcik.pdf

[15] OVAL, Open Vulnerability and Assessment Language, http://oval.mitre.org/

[16] XCCDF, The eXtensible Configuration Checklist Description Format, http://scap.nist.gov/specifications/xccdf/

[17] CRF, Common Result Format: http://makingsecuritymeasurable.mitre.org/crf/

[18] IODEF, Incident Object Description and Exchange Format, http://xml.coverpages.org/iodef.html

[19] VerIS, The Verizon Incident Sharing Framework, http://securityblog.verizonbusiness.com/wp-content/uploads/2010/03/VerIS_Framework_Beta_1.pdf

[20] CEE, Common Event Expression, http://cee.mitre.org/

[21] H. Debar, D. Curry, B. Feinstein, The Intrusion Detection Message Exchange Format (IDMEF), IETF RFC 4765, 2007**.**

[22] NASL, Nessus Attack Scripting Language, http://www.nessus.org/

[23] Snort Rules, http://www.snort.org/snort-rules/

[24] Regex, Regular expressions, http://en.wikipedia.org/wiki/Regular_expression

[25] ISO/IEC 27005:2008, Information technology -- Security techniques -- Information security risk management, http://ww.iso.org,; http://www.27000.org/iso-27005.htm

[26] ISO 8601:2004, Data elements and interchange formats - Information interchange - Representation of dates and times, http://ww.iso.org, http://en.wikipedia.org/wiki/ISO_8601